(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10224763 A**

(43) Date of publication of application: **21 . 08 . 98**

(51) Int. Cl **H04N 7/167**
H04L 9/14

(21) Application number: **09023551**

(22) Date of filing: **06 . 02 . 97**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

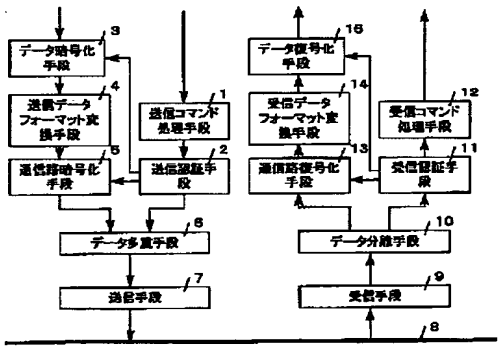
(72) Inventor: **YANAGAWA YOSHIFUMI**
MATSUMI CHIYOKO
YOSHIDA JUNJI
KOBAYASHI MASAAKI
NAGAOKA YOSHITOMI

(54) **CIPHERING DEVICE, DECIPHERING DEVICE AND CIPERING/ DECIPHERING DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To attain ciphering corresponding to transmitting/receiving data by providing the system with a data ciphering means, a communication line ciphering means, a data deciphering means, and a communication line deciphering means.

SOLUTION: The data ciphering means 3 ciphers AV data consisting of video data and voice data and allowed to be transmitted by a data transmission key received from a transmission certificating means 2 and outputs ciphered transmitting data. The communication line ciphering means 5 ciphers synchronizing transmitting data by a communication transmission key outputted from the means 2 and outputs the ciphered data to a data multiplexing means 6 as ciphered synchronizing transmitting data. On the other hand, the communication line deciphering means 13 receives a communication reception key from a reception certificating means 11, deciphers the ciphered synchronizing receiving data by the communication reception key and generates synchronizing receiving data. The data deciphering means 15 deciphers the ciphered receiving data by a data reception key and generates receiving data. Consequently strong ciphering can be applied only to transmitting/receiving data having high secrecy.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－224763

(43)公開日　平成10年(1998)８月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１

審査請求　未請求　請求項の数10　ＯＬ　（全 14 頁）

(21)出願番号　特願平9－23551

(22)出願日　平成９年(1997)２月６日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　柳川　良文
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　松見　知代子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　▲吉▼田　順二
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　滝本　智之　（外１名）

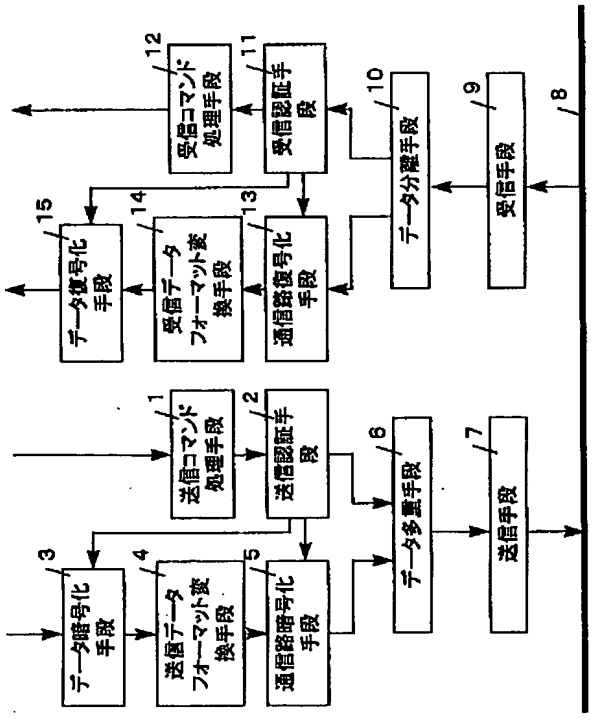
最終頁に続く

(54)【発明の名称】　暗号化装置および復号化装置および暗号化復号化装置

(57)【要約】

【課題】　送受信データの種類や内容により暗号化の強度を変更可能にし、映像の種類や映像データの圧縮形式等に対して柔軟に暗号化を変更可能にする。

【解決手段】　データ用送信キーで送信データを暗号化するデータ暗号化手段３と、データ暗号化手段３の出力の暗号化送信データを同期送信データに変換する送信データフォーマット変換手段４と、通信用送信キーで同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段５と、通信用受信キーで暗号化同期受信データを復号する通信路復号化手段１３と、通信路復号化手段１３の出力を変換して暗号化受信データを生成する受信データフォーマット変換手段１４と、データ用受信キーを用いて暗号化受信データの復号を行い受信データを生成するデータ復号化手段１５とを備え、通信路８の暗号化とは独立して、送受信データの種類や内容に応じてデータの暗号化強度を任意に設定する。



1

【特許請求の範囲】

【請求項１】　送信制御信号を処理する送信コマンド処理手段と、
前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
前記送信認証手段が出力するデータ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、
前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、
前記送信認証手段が出力する通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
前記データ多重手段の出力する通信用データを通信路上に送出する送信手段と、
前記通信路から通信用データを受信する受信手段と、
前記通信用データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、
前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号手段とを備える暗号化復号化装置。

【請求項２】　送信制御信号を処理する送信コマンド処理手段と、
前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
前記送信認証手段が出力するデータ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、
前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、
前記送信認証手段が出力する通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
前記データ多重手段の出力する通信用送信データを通信路上に送出する送信手段とを備える暗号化装置。

【請求項３】　通信路から通信用受信データを受信する受信手段と、

2

前記通信用受信データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、
前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号手段とを備える復号化装置。

【請求項４】　送信制御信号を処理する送信コマンド処理手段と、
前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
前記送信認証手段が出力するデータ用送信キーを用いて送信データを暗号化する複数のデータ暗号化手段と、
前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、
前記送信認証手段が出力する通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
前記データ多重手段の出力する通信用データを通信路上に送出する送信手段と、
前記通信路から通信用データを受信する受信手段と、
前記通信用データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、
前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号手段とを備える暗号化復号化装置。

【請求項５】　送信制御信号を処理する送信コマンド処理手段と、
前記送信コマンド処理手段に接続されデータ送信時の認証処理を行う送信認証手段と、
前記送信認証手段が出力するデータ用送信キーを用いて

送信データを暗号化する複数のデータ暗号化手段と、
前記データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、
前記送信認証手段が出力する通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、
前記暗号化同期送信データと前記送信認証手段が出力する非同期送信データとを多重化するデータ多重手段と、
前記データ多重手段の出力する通信用送信データを通信路上に送出する送信手段とを備える暗号化装置。

【請求項６】　通信路から通信用受信データを受信する受信手段と、
前記通信用受信データを暗号化同期受信データと非同期受信データとに分離するデータ分離手段と、
前記データ分離手段に接続されデータ受信時の認証処理を行う受信認証手段と、
前記受信認証手段の出力する受信制御信号を処理する受信コマンド処理手段と、
前記受信認証手段が出力する通信用受信キーを用いて前記暗号化同期受信データを復号する通信路復号手段と、
前記通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、
前記受信認証手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号手段とを備える復号化装置。

【請求項７】　受信データ及び送信データは、映像データ及び音声データからなるＡＶデータであることを特徴とする請求項１ないし６のいずれかに記載の暗号化装置および復号化装置および暗号化復号化装置。

【請求項８】　映像データはプログレッシブ映像データであることを特徴とする請求項７記載の暗号化装置および復号化装置および暗号化復号化装置。

【請求項９】　送信データフォーマット変換手段は、送信認証手段が出力するデータ用受信キー及びデータ暗号化手段が出力する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換することを特徴とする請求項１、２、４または５のいずれかに記載の暗号化装置および暗号化復号化装置。

【請求項１０】　受信データフォーマット変換手段は、通信路復号手段が出力する同期受信データのフォーマット変換を行い暗号化受信データ及びデータ用受信キーを生成し、
データ復号手段は、前記受信データフォーマット変換手段が出力するデータ用受信キーを用いて前記暗号化受信データの復号を行うことを特徴とする請求項１、３、４または６のいずれかに記載の復号化装置および暗号化復号化装置。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明は、映像機器やオーディオ機器をネットワーク上に接続し、映像及び音声データをネットワークを経由して伝送するネットワークインターフェース装置に関し、特に、ネットワーク上に流す映像及び音声データを変換加工して暗号化するとともに、ネットワーク上から受け取ったデータを変換加工して映像及び音声データに復号化する暗号化装置および復号化装置および暗号化復号化装置に関するものである。

【０００２】
【従来の技術】近年、ケーブルテレビジョンや通信衛星を用いて、映像データ及び音声データを配信するサービスが開始されており、これらを受信するためのセットトップボックスや家庭用ディジタルビデオカメラ等のＡＶ機器にもネットワークインターフェースをもつ機器が普及してきている。これらの機器をネットワークで接続する際、著作権や課金等の問題により、映像及び音声データに対する暗号化復号化装置が必要とされてきている。

【０００３】従来、暗号化復号化装置として、例えば特開平６－１２５５５４号公報に記載されているものがあり、暗号化復号化装置に用いられるいくつかの技術を開示している。以下に図面を参照しながら、従来の暗号化復号化装置の一例について説明する。

【０００４】図８は従来の暗号化復号化装置の一例を示すものである。図８において、１は送信コマンド処理手段、２は送信認証手段、４は送信データフォーマット変換手段、５は通信路暗号化手段、６はデータ多重手段、７は送信手段、８は通信路、９は受信手段、１０はデータ分離手段、１１は受信認証手段、１２は受信コマンド処理手段、１３は通信路復号化手段、１４は受信データフォーマット変換手段である。

【０００５】ここで、ネットワーク上へ送信する場合、送信コマンド処理手段１は送信先名や機器制御コマンド等からなるコマンド入力を受け、このコマンド入力を送信相手に理解できる制御情報に変換するとともに、送信認証手段２に対して送信データの認証及び通信路の認証を要求する。送信認証手段２は、例えば、本装置内に記憶させている送信先の公開キーを通信用送信キーとして通信路暗号化手段５へ出力するとともに、送信コマンド処理手段１から受け取った制御情報を非同期送信データとしてデータ多重手段６へ出力する。

【０００６】一方、映像データや音声データ等からなる送信データは、送信データフォーマット変換手段４で通信路８のデータフォーマットの同期送信データに変換され、通信路暗号化手段５へ出力される。通信路暗号化手段５ではこの同期送信データを通信用送信キーで暗号化し暗号化同期送信データとしてデータ多重手段６へ出力する。

【０００７】データ多重手段６は非同期送信データ及び暗号化同期送信データを時分割等の手段で多重化し、送

信手段７はこのデータを通信路８へ送信する。データをネットワーク上から受信する場合、受信手段９は通信路８よりデータを受信し、データ分離手段１０で時分割多重されたデータを分離し、暗号化同期受信データ及び非同期受信データを生成する。

【０００８】受信認証手段１１は非同期受信データから制御情報を抽出するとともに、本装置内に記憶されている秘密キーを通信用受信キーとして通信路復号化手段１３へ出力する。ここで、受信された制御情報は受信コマンド処理手段１２で処理され、本装置内部で有効なコマンドを生成する。一方、通信路復号化手段１３は受信認証手段１１から通信用受信キーを受け取り、暗号化同期受信データをこの通信用受信キーで復号して同期受信データを生成する。受信データフォーマット変換手段１４は同期受信データのフォーマット変換を行い、受信データを生成する。

【０００９】このようにして、ネットワーク上にある送信先以外の機器に対しては、送信情報を隠匿する。

【００１０】

【発明が解決しようとする課題】しかしながら上記のような構成では、通信路の暗号化手法により暗号化の強度が決まってしまい、送受信するデータの内容によって暗号化の強度を変えることができないという問題点を有していた。本発明は上記問題点を解決するもので、送受信データにより暗号化の強度を変更可能にし、送受信データとして用いる映像データの種類、内容や圧縮形式等に対して柔軟に暗号化方法を変更できる暗号化復号化装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記問題点を解決するために本発明の暗号化復号化装置は、データ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号手段とを具備することを特徴とするものである。

【００１２】また、データ用送信キーを用いて送信データを暗号化する複数のデータ暗号化手段と、各々のデータ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号手段とを具備することを特徴とするものである。

【００１３】そして、送信データ及び受信データは映像データ又は音声データ等からなるＡＶデータであることを特徴とするものである。さらに、映像データをノンインターレス方式のプログレッシブ画像データとすることを特徴とするものである。また、データ用受信キーは暗号化送信データ及び暗号化受信データの一部として送受信することを特徴とするものである。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態による暗号化復号化装置について、図面を参照しながら説明する。

（実施の形態１）図１は本発明の実施の形態１における暗号化復号化装置のブロック図を示すものである。ここで、従来例と同一の構成要素には同一の符号を付し説明を省略する。

【００１５】図１において、１は送信コマンド処理手段、２は送信認証手段、３はデータ暗号化手段、４は送信データフォーマット変換手段、５は通信路暗号化手段、６はデータ多重手段、７は送信手段、８は通信路、９は受信手段、１０はデータ分離手段、１１は受信認証手段、１２は受信コマンド処理手段、１３は通信路復号化手段、１４は受信データフォーマット変換手段、１５はデータ復号化手段である。

【００１６】ここで、ネットワーク上へ送信する場合、送信コマンド処理手段１は送信先名や機器制御コマンド等からなるコマンド入力を受け、このコマンド入力を送信相手に理解できる制御情報に変換するとともに、送信認証手段２に対して送信データの認証及び通信路の認証を要求する。この機器制御コマンドは、例えば本装置をＶＴＲやレーザーディスクに組み込むのであれば再生、サーチ等の制御情報であり、これらの情報を受信機器との間で規定したコードに変換し、送信認証手段２へ出力する。

【００１７】送信認証手段２は、例えば、本装置内に記憶されている送信先の公開キーを通信用送信キーとして通信路暗号化手段５へ、また、送信データ用の公開キーをデータ用送信キーとしてデータ暗号化手段３へ出力するとともに、送信コマンド処理手段１から受け取った制御情報を非同期送信データとしてデータ多重手段６へ出力する。ここで、必ずしも送信データ用の公開キーや送信先の公開キーをデータ用送信キーや通信用送信キーとして用いる必要はなく、映像等の送信データを送信する

前に送信認証手段２において、非同期データを送受信することにより送信先から暗号化キーを取得しても良いし、本装置に記憶してある秘密キーや乱数により生成した秘密キーを暗号化キーとして用いて暗号化し、この秘密キーに対する公開キーを送信先にのみ非同期データとして送信しても良い。

【００１８】さらに、送信先の複数の機器に共通のキーを設定し、このキーの公開キーまたは秘密キーのいずれかを用いて暗号化しても良い。また、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、このキーをデータ用送信キーとして用いてもよい。さらに、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いても良い。さらに、データ用送信キー及びデータ用受信キーは地上波ＴＶ放送、ＣＡＴＶ、ディジタルＴＶ放送、ディジタル衛星放送や電話回線等の通信回線を通して受け取ったものとしてもよく、例えば、ＴＶ放送等からＶＴＲ等に録画したＡＶデータに対して、ＶＴＲ等で再生する際に、ＴＶ放送等からＶＴＲ録画時又はＶＴＲ再生時に受け取ったデータ用送信キーで暗号化し、通信路上にある表示機器では装着されているスマートカードに記憶されているデータ用受信キーや電話回線を通して受け取ったデータ用受信キーで復号するとしても良い。

【００１９】ここでは、秘密キーと公開キーによる暗号化で説明したが、暗号化復号化を一つのキーで行っても良い。一方、データ暗号化手段３は映像データや音声データからなる送信すべきＡＶデータ（送信データ）を送信認証手段２から受け取ったデータ用送信キーで暗号化し、暗号化送信データを生成する。

【００２０】次に、送信データフォーマット変換手段４は暗号化送信データを通信路のデータフォーマット形式の同期送信データに変換し、通信路暗号化手段５へ出力する。ここで、送信データは、例えばディジタルＶＴＲで使用されているＤＶデータ形式やＭＰＥＧデータ形式のものであり、同期送信データは、例えばＩＥＥＥ１３９４－１９９５で規定されたアイソクロナスパケットの形式のものである。

【００２１】通信路暗号化手段５ではこの同期送信データを、送信認証手段２が出力する通信用送信キーで暗号化し暗号化同期送信データとしてデータ多重手段６へ出力する。データ多重手段６は、例えばＩＥＥＥ１３９４－１９９５に規定された方法を用いて、非同期送信データはアシンクロナスパケットとして、暗号化同期送信データはアイソクロナスパケットとして多重化する。もちろん、ここで、非同期データの転送レートが十分にあれば、時分割多重等の方法で多重化し非同期パケットとして送信しても良い。

【００２２】送信手段７は通信路８のバスアービトレーションを行い、バスの使用権を獲得し、アシンクロナスパケットを送信先に転送するとともに、アイソクロナスパケットに対しては、例えばＩＥＥＥ１３９４－１９９５プロトコルに則り、ある時間周期で周期的に送信先へ送信する。次に、ネットワーク上からデータを受信する場合、受信手段９は通信路８より、例えば、自分宛のアシンクロナスパケット及びアイソクロナスパケットを受信し、データ分離手段１０において多重化されたデータを分離し、アシンクロナスパケットから非同期受信データを、アイソクロナスパケットから暗号化同期受信データを取得する。

【００２３】受信認証手段１１は非同期受信データから制御情報を抽出するとともに、本装置内に記憶されている秘密キーを通信用受信キーとして通信路復号化手段１３へ、受信データ用の秘密キーをデータ用受信キーとしてデータ復号化手段１５へ出力する。さらに、受信された制御情報は受信コマンド処理手段１２で処理され、本装置内部で有効なコマンドを生成する。ここで、通信用受信キー及びデータ用受信キーは必ずしも秘密キーである必要はなく、送信認証手段２の説明で述べたのと同様な方法を用いることが可能である。

【００２４】一方、通信路復号化手段１３は受信認証手段１１から通信用受信キーを受け取り、暗号化同期受信データをこの通信用受信キーで復号して同期受信データを生成する。受信データフォーマット変換手段１４は同期受信データのフォーマット変換を行い、暗号化受信データを生成する。ここで、同期送信データは、例えばＩＥＥＥ１３９４－１９９５で規定されたアイソクロナスパケットの形式のものであり、暗号化受信データは、例えばディジタルＶＴＲで使用されているＤＶデータ形式のデータを暗号化したものである。

【００２５】データ復号化手段１５は、暗号化受信データをデータ用受信キーで復号し、受信データを生成する。この受信データは、例えばディジタルＶＴＲで使用されているＤＶデータである。よって、データ復号化手段１５の出力信号を所望の時間間隔でＤＶエンコーダ等に入力することにより、ＮＴＳＣ映像データを得られ、例えばＴＶ画面上に表示することが可能となる。ここで、映像データはＮＴＳＣ映像データとしたが、ノンインターレス方式のプログレッシブ画像データとしてもよく、この時パーソナルコンピュータ上でも高画質な映像データを容易に表示可能になるとともに、プログレッシブ画像データに対して課金等のために必要な暗号化を適切かつ容易に実現できる。また、パーソナルコンピュータ等が接続され、これらがデータ受信キーを持たず、データを盗聴加工する可能性のある場合、プログレッシブ画像データに対しては解読しにくい暗号化を行うことも可能であり、送受信データの安全性を高めることができる。

【００２６】以上のように本実施の形態のよれば、データ暗号化手段、通信路暗号化手段、データ復号化手段及

び通信路復号化手段を用いることにより、送受信データに応じた暗号化を行うことができ、隠匿性の高い送受信データに対してのみ強い暗号化を行うことが容易に実現可能になり、送受信データの内容に応じて柔軟に暗号化強度を変更することが可能になる。

【００２７】また、送受信データとして、映像データや音声データからなるＡＶデータを用いることにより、ペイパービューの映像に対しては見にくいが何の映像であるかは大体理解できるような暗号化を行うことや秘密性の高い映像に対しては強力な暗号化を行うことが可能となり、映像や音声等の内容に応じて暗号化強度を変更できる。

【００２８】さらに、ＴＶ放送等からＶＴＲ等に録画したＡＶデータに対して、ＶＴＲ等で再生する際に暗号化することが可能になり、通信路上に接続された表示機器でこのＡＶデータを視聴することに対して著作権の保護や課金等を行うことができる。なお、本実施の形態においてデータ暗号化手段等からなるデータ送信部とデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、データ用送信キー及びデータ用受信キーをあらかじめ設定しておけば、例えば、映像の再生専用機器においては送信コマンド処理手段、送信認証手段、データ暗号化手段、送信データフォーマット変換手段、通信路暗号化手段、データ多重化手段、送信手段からなるデータ送信部のみを内蔵すればよく、また、モニタのように映像データの受信のみを行う機器では受信コマンド処理手段、受信認証手段、データ復号化手段、受信データフォーマット変換手段、通信路復号化手段、データ分離化手段、受信手段からなるデータ受信部のみを内蔵すればよい。

【００２９】また、本実施の形態では送信データ及び受信データは映像データや音声データからなるＡＶデータであるとしたが、秘密性のある各種データ（例えば、文書データや表データ）に対しても適用可能であり、同様の効果が得られる。そして、本実施の形態で示した各手段は送信手段及び受信手段の通信路ドライブ回路等を除きソフトウエアで実現しても同様の効果が得られる。

【００３０】さらに、データ多重手段及び送信手段は一つの手段で構成しても良く、同様の効果が得られる。これはデータ分離手段及び受信手段に関しても同様である。図２は本実施の形態において、送信コマンド処理手段１と受信コマンド処理手段１２を送受信コマンド処理手段１６で、送信認証手段２と受信認証手段１１を送受信コマンド処理手段１７で実現した場合のブロック図である。このように構成することにより、送信側と受信側で非同期データをやり取りし、データの送受信、特に非同期データの送受信に必要な認証や機器制御等を行うことが容易になり、種々の機器が通信路８上につながる場合にも柔軟に対応できる。例えば、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、このキーをデータ用送信キーとして用いて暗号化することや、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いて暗号化することも容易になる。

【００３１】ここではデータ暗号化手段等からなるデータ送信部とデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、例えば、映像の再生専用機器においては図３に示すように、送受信コマンド処理手段１６、送受信認証手段１７、データ暗号化手段３、送信データフォーマット変換手段４、通信路暗号化手段５、データ多重化手段６、送信手段７からなるデータ送信部と送受信認証手段１７に接続された非同期データ用の受信手段９のみを用いて暗号化装置を構成すればよい。

【００３２】また、モニタのように映像データの受信のみを行う機器では図４に示すように送受信コマンド処理手段１６、送受信認証手段１７、データ復号化手段１５、受信データフォーマット変換手段１４、通信路復号化手段１３、データ分離化手段１０、受信手段９からなるデータ受信部と送受信認証手段１７に接続された非同期データ用の送信手段７のみを用いて復号化装置のみを構成すればよい。

【００３３】図５は本実施の形態において、データ用送信キーを同期送信データとともに送信し、データ用受信キーを同期受信データとともに受信する場合の例である。ここで、まず、送信認証手段２は、例えば、本装置内に記憶されている送信先の公開キーを通信用送信キーとして通信路暗号化手段５へ、また、送信データ用の公開キーをデータ用送信キーとしてデータ暗号化手段３へ出力するとともに、送信データ用の秘密キーをデータ用受信キーとして送信データフォーマット変換手段４へ出力する。ここで、必ずしも送信データ用の公開キーや秘密キーをデータ用送信キーやデータ用受信キーとして用いる必要はなく、本装置に記憶してある秘密キーや乱数により生成した秘密キーをデータ用送信キーとして用いて暗号化し、この秘密キーに対する公開キーをデータ用受信キーとして用いても良い。さらに、送信先の複数の機器に共通のキーを設定し、このキーの公開キーと秘密キーをデータ用送信キー及びデータ用受信キーとして用いても良い。また、ここでは秘密キーと公開キーによる暗号化で説明したが、暗号化／復号化を一つのキーで行っても良く、この時、データ暗号化手段３及び送信データフォーマット変換手段４へ出力するキーは同一のものとなる。このように構成することにより、データ用受信キーの取り扱いが容易になり、通信路の秘密性を確保しつつ送受信データに対して適切な暗号化を簡単な構成で実現できる。

【００３４】次に、送信データフォーマット変換手段４はデータ暗号化手段３の出力する暗号化送信データ及び

データ用受信キーを通信路のデータフォーマット形式の同期送信データに変換し、通信路暗号化手段５へ出力する。一方、受信データフォーマット変換手段１４は同期受信データのフォーマット変換を行い、暗号化受信データ及びデータ用受信キーを抽出する。このデータ用受信キーを用いて、データ復号化手段１５は暗号化受信データを復号し、受信データを生成する。このように構成することで、データ用受信キーをあらかじめ受信側の装置内に保持する必要なくなり、構成を簡単化できるとともに、通信路の安全は通信路の暗号化により確保することが可能である。

【００３５】（実施の形態２）以下本発明の実施の形態２について図面を参照しながら説明する。図６、図７は本発明の実施の形態２を示す暗号化復号化装置のブロック図である。ここで、実施の形態１と同一の構成要素には同一の符号を付し説明を省略する。図６において、２０は第１のデータ暗号化手段、２１は第１の送信データフォーマット変換手段、２２は第Ｎのデータ暗号化手段、２３は第Ｎの送信データフォーマット変換手段、３０は第１のデータ復号化手段、３１は第１の受信データフォーマット変換手段、３２は第Ｎのデータ復号化手段、３３は第Ｎの受信データフォーマット変換手段である。但し、ここで、Ｎは自然数であり、Ｎ個のデータ暗号手段及び送信データフォーマット変換手段があることを示している。本実施の形態では第１のデータ暗号化手段と第Ｎのデータ暗号化手段等の２つを用いた場合で説明しているが、任意の自然数Ｎ個のデータ暗号化手段等を用いた場合も本実施の形態と同様の手法で実現可能である。

【００３６】まず、ネットワーク上へ送信する場合、送信認証手段２は、例えば、本装置内に記憶されている送信先の公開キーを通信用送信キーとして通信路暗号化手段５へ、また、第１のストリームデータ用の公開キーを第１のデータ用送信キーとして第１のデータ暗号化手段２０へ、第Ｎの送信データ用の公開キーを第Ｎのデータ用送信キーとして第Ｎのデータ暗号化手段２２へ出力するとともに、送信コマンド処理手段１から受け取った制御情報を非同期送信データとしてデータ多重手段６へ出力する。

【００３７】なお、第１のデータ用送信キーと第Ｎのデータ用送信キーとは異なっていてもよいし同一でもよい。ここで、実施の形態１と同様に、必ずしも送信データ用の公開キーや送信先の公開キーをデータ用送信キーや通信用送信キーとして用いる必要はなく、映像等の送信データを送信する前に送信認証手段２において、非同期データを送受信することにより送信先から暗号化キーを取得しても良いし、本装置に記憶してある秘密キーや乱数により生成した秘密キーを暗号化キーとして用いて暗号化し、この秘密キーに対する公開キーを送信先にのみ非同期データとして送信しても良い。さらに、送信先の複数の機器に共通のキーを設定し、このキーの公開キーを用いて暗号化しても良い。

【００３８】また、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、このキーをデータ用送信キーとして用いてもよい。さらに、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いても良い。さらに、データ用送信キー及びデータ用受信キーは地上波ＴＶ放送、ＣＡＴＶ、ディジタルＴＶ放送、ディジタル衛星放送や電話回線等の通信回線を通して受け取ったものとしてもよく、例えば、ＴＶ放送等からＶＴＲ等に録画したＡＶデータに対して、ＶＴＲ等で再生する際に、ＴＶ放送等からＶＴＲ録画時又はＶＴＲ再生時に受け取ったデータ用送信キーで暗号化し、通信路上にある表示機器では装着されているスマートカードに記憶されているデータ用受信キーや電話回線を通して受け取ったデータ用受信キーで復号するとしても良い。

【００３９】ここでは、秘密キーと公開キーによる暗号化で説明したが、暗号化復号化を一つのキーで行っても良い。一方、第１のデータ暗号化手段２０及び第Ｎのデータ暗号化手段２２は映像データや音声データからなる送信すべき送信データを送信認証手段２から受け取ったデータ用送信キーで暗号化し、暗号化送信データを生成する。ここで、第１のデータ暗号化手段２０には第１の送信データが入力され、第Ｎのデータ暗号化手段２２には第Ｎの送信データが入力される。例えば、第１の送信データはディジタルＶＴＲで使用されているＤＶデータであり、第Ｎの送信データはディジタル衛星放送等で使用されているＭＰＥＧデータであるとする。この時、第１のデータ暗号化手段２０では、第１のデータ用送信キーですべてのフレームを同じ暗号化方式で暗号化し、第Ｎのデータ暗号化手段２２では、第Ｎのデータ用送信キーでＭＰＥＧデータ中のＩフレームのみに対して暗号化する。ここで、もちろん、第１のデータ暗号化手段２０と第Ｎのデータ暗号化手段２２で同一の暗号化をしてもかまわない。

【００４０】次に、第１の送信データフォーマット変換手段２１及び、第Ｎの送信データフォーマット変換手段２３は暗号化送信データを通信路のデータフォーマット形式の第１の同期送信データ及び第Ｎの同期送信データに変換し、通信路暗号化手段５へ出力する。ここで、同期送信データは、例えばＩＥＥＥ１３９４－１９９５で規定されたアイソクロナスパケットの形式のものである。

【００４１】通信路暗号化手段５ではこれらの同期送信データを、送信認証手段２が出力する通信用送信キーで暗号化し暗号化同期送信データとしてデータ多重手段６へ出力する。データ多重手段６は、例えばＩＥＥＥ１３９４－１９９５に規定された方法を用いて、非同期送信

データはアシンクロナスパケットとして、暗号化同期送信データはアイソクロナスパケットとして多重化する。

【００４２】送信手段７は通信路８のバスアービトレーションを行い、バスの使用権を獲得し、アシンクロナスパケットを送信先に転送するとともに、アイソクロナスパケットに対しては、例えばＩＥＥＥ１３９４－１９９５プロトコルに則り、ある時間周期で周期的に送信先へ送信する。次に、ネットワーク上からデータを受信する場合、受信手段９は通信路８より自分宛のアシンクロナスパケット及びアイソクロナスパケットを受信し、データ分離手段１０で多重化されたデータを分離し、アシンクロナスパケットから非同期受信データを、アイソクロナスパケットから暗号化同期受信データを取得する。

【００４３】受信認証手段１１は非同期受信データから制御情報を抽出するとともに、本装置内に記憶されている秘密キーを通信用受信キーとして通信路復号化手段１３へ、送信データ用の秘密キーをデータ用受信キーとしてデータ復号化手段１５へ出力する。さらに、受信された制御情報は受信コマンド処理手段１２で処理され、本装置内部で有効なコマンドを生成する。ここで、通信用受信キー及びデータ用受信キーは必ずしも秘密キーである必要はなく、送信認証手段２の説明で述べたのと同様の方法を用いることが可能である。

【００４４】一方、通信路復号化手段１３は受信認証手段１１から通信用受信キーを受け取り、暗号化同期受信データをこの通信用受信キーで復号して同期受信データを生成する。第１の受信データフォーマット変換手段３１及び第Ｎの受信データフォーマット変換手段３３は同期受信データのフォーマット変換を行い、各々第１の暗号化受信データ及び第Ｎの暗号化受信データを生成する。ここで、例えば、第１の暗号化受信データはＤＶデータ形式のデータを暗号化したものであり、第Ｎの暗号化受信データはＭＰＥＧデータ形式のデータを暗号化したものである。また、同期送信データは、例えばＩＥＥＥ１３９４－１９９５で規定されたアイソクロナスパケットの形式のものである。

【００４５】第１のデータ復号化手段３０及び第Ｎのデータ復号化手段３２は、暗号化受信データを各々第１のデータ用受信キー及び第Ｎのデータ用受信キーで復号し、第１の受信データ及び第Ｎの受信データを生成する。例えば、第１の受信データはＤＶデータであり、第Ｎの受信データはＭＰＥＧデータである。これらの受信データを所望の時間間隔でＤＶエンコーダ及びＭＰＥＧエンコーダへ各々入力することにより映像データを得られ、例えばモニター画面上に表示することが可能となる。ここで、映像データをノンインターレス方式のプログレッシブ画像データとしてもよく、この時パーソナルコンピュータ上でも高画質な映像データを容易に表示可能になるとともに、プログレッシブ画像データに対して課金等のために必要な暗号化を適切かつ容易に実現できる。また、パーソナルコンピュータ等が接続され、これらがデータ受信キーを持たず、データを盗聴加工する可能性のある場合、プログレッシブ画像データに対しては解読しにくい暗号化を行うことも可能であり、送受信データの安全性を高めることができる。

【００４６】以上のように本実施の形態のよれば、複数のデータ暗号化手段と複数の送信フォーマット変換手段と通信路暗号化手段を用いることにより、ストリームデータに応じた暗号化を行うことができ、例えば、ＤＶ形式で圧縮された映像データやＭＰＥＧ形式で圧縮された映像データに対して、各々適切な暗号化を行える。よって、映像情報に対して必要とされる隠匿性を、各々の映像データの圧縮形式で適切な方法で暗号化でき、暗号化が容易となる。例えば、ネットワーク上にあり、通信用受信キーはあるが、データ用受信キーを持たない機器でも、見にくいが何の映像であるかは大体理解できるような映像を画像の圧縮形式に依存せず簡単に暗号化することが可能となる。

【００４７】なお、本実施の形態では複数の送信データフォーマット変換手段はデータ多重化手段に接続されているとしたが、複数の送信データフォーマット変換手段をスイッチで切り替え、このうち一つを選択して、データ多重手段に接続しても良く、スイッチの切り替えを送信コマンド処理手段や送信認証手段で制御する必要があるが同様の効果が得られる。これは、複数の受信データフォーマット変換手段に対しても同様である。

【００４８】また、本実施の形態では第１のデータ暗号化手段等からなるデータ送信部と第１のデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、各々の送受信データに対してデータ用送信キー及びデータ用受信キーをあらかじめ設定しておけば、例えば、映像の再生専用機器においては送信コマンド処理手段、送信認証手段、第１のデータ暗号化手段、第Ｎのデータ暗号化手段、第１の送信データフォーマット変換手段、第Ｎの送信データフォーマット変換手段、通信路暗号化手段、データ多重化手段、送信手段からなるデータ送信部のみを用いればよく、また、モニタのように映像データの受信のみを行う機器では受信コマンド処理手段、受信認証手段、第１のデータ復号化手段、第Ｎのデータ復号化手段、第１の受信データフォーマット変換手段、第Ｎの受信データフォーマット変換手段、通信路復号化手段、データ分離化手段、受信手段からなるデータ受信部のみを用いればよい。

【００４９】そして、本実施の形態で示した各手段は送信手段及び受信手段の通信路ドライブ回路等を除きソフトウエアで実現しても同様の効果が得られる。また、データ多重手段及び送信手段は一つの手段で構成しても良く、同様の効果が得られる。これはデータ分離手段及び受信手段に関しても同様である。さらに、本実施の形態においても図２で示したのと同様に、送信コマンド処理

手段１と受信コマンド処理手段１２を送受信コマンド処理手段１６で、送信認証手段２と受信認証手段１１を送受信コマンド処理手段１７で実現することも可能であり、例えば、受信先から秘密キーまたは公開キーを非同期データ等により受け取り、このキーをデータ用送信キーとして用いて暗号化することや、非同期データ等の通信により送信側と受信側で秘密キーまたは公開キーを取り決め、これらのキーのいずれかをデータ用送信キーとして用いて暗号化することも容易になる。

【００５０】ここでは第１のデータ暗号化手段等からなるデータ送信部と第１のデータ復号化手段等からなるデータ受信部を一つの装置に内蔵するとしたが、例えば、映像の再生専用機器においては図３と同様にして、送受信コマンド処理手段１６、送受信認証手段１７、第１のデータ暗号化手段２０、第Ｎのデータ暗号化手段２２、第１の送信データフォーマット変換手段２１、第Ｎの送信データフォーマット変換手段２３、通信路暗号化手段１５、データ多重化手段６、送信手段７からなるデータ送信部と送受信認証手段１７に接続された非同期データ用の受信手段９のみを用いて暗号化装置を構成すればよい。また、モニタのように映像データの受信のみを行う機器では図４と同様にして、送受信コマンド処理手段１６、送受信認証手段１７、第１のデータ復号化手段３０、第Ｎのデータ復号化手段３２、第１の受信データフォーマット変換手段３１、第Ｎの受信データフォーマット変換手段３３、通信路復号化手段１３、データ分離化手段１０、受信手段９からなるデータ受信部と送受信認証手段１７に接続された非同期データ用の送信手段７のみを用いて復号化装置を構成すればよい。

【００５１】また、本実施の形態においても図５で示したのと同様に、データ用送信キーを同期送信データとともに送信し、データ用受信キーを同期受信データとともに受信することも可能であり、データ用受信キーの取り扱いを容易にでき、通信路の秘密性を確保しつつ送受信データに対して適切な暗号化を簡単な構成で実現できる。

【００５２】

【発明の効果】以上のように本発明によれば、データ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号化手段とを具備することにより、送受信データの内容や種類に応じた暗号化を行うことができ、隠匿性の高い送受信データに対しては強い暗号化を行うことが容易となる。

【００５３】また、データ用送信キーを用いて送信データを暗号化する複数のデータ暗号化手段と、各々のデータ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する複数の送信データフォーマット変換手段と、通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する複数の受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成する複数のデータ復号化手段とを具備することにより、各種の送受信データに各々応じた暗号化を行うことができ、複数の送受信データに対して柔軟に暗号化強度を変更できる。

【００５４】そして、データ用送信キーを用いて送信データを暗号化するデータ暗号化手段と、データ暗号化手段が生成する暗号化送信データを通信路用データフォーマットを有する同期送信データに変換する送信データフォーマット変換手段と、通信用送信キーを用い前記同期送信データを暗号化して暗号化同期送信データを生成する通信路暗号化手段と、通信用受信キーを用いて暗号化同期受信データを復号する通信路復号化手段と、前記通信路復号化手段が出力する同期受信データのフォーマット変換を行い暗号化受信データを生成する受信データフォーマット変換手段と、データ用受信キーを用いて前記暗号化受信データの復号を行い受信データを生成するデータ復号化手段とを具備し、送信データ及び受信データは映像データ又は音声データ等のＡＶデータであるとすることにより、各々のＡＶデータに対して必要とされる隠匿性を、各々の映像データの圧縮形式等に対して適切な方法で暗号化でき、暗号化が容易となる。よって、ネットワーク上にあり、通信用受信キーはあるが、データ用受信キーを持たない機器でも、見にくいが何の映像であるかは大体理解できるような映像を画像の圧縮形式に応じて簡単に暗号化することが可能となる。また、ＴＶ放送等からＶＴＲ等に録画したＡＶデータに対して、ＶＴＲ等で再生する際に暗号化することが可能になり、著作権の保護や課金等を行うことができる。

【００５５】さらに、映像データをノンインターレス方式のプログレッシブ画像データとすることにより、パーソナルコンピュータ上でも高画質な映像データを容易に表示可能になるとともに、プログレッシブ画像データに対して課金等のために必要な暗号化を適切かつ容易に実現できる。また、パーソナルコンピュータ等が接続され、これらがデータ受信キーを持たず、データを盗聴加

工する可能性のある場合、プログレッシブ画像データに対しては解読しにくい暗号化を行うことも可能であり、送受信データの安全性を高めることができる。

【００５６】また、データ用送信キー及び受信キーを暗号化送信データ及び暗号化受信データの一部として送受信し、通信用送信キー及び通信用受信キーを用いて通信路の暗号化を行うことにより、通信路の安全性を確保した上で、各々の送受信データに対して適切な暗号化を容易に行うことができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１における暗号化復号化装置のブロック図

【図２】同暗号化復号化装置において送受信認証手段を用いた場合のブロック図

【図３】同暗号化復号化装置において送受信認証手段を用いた場合のブロック図

【図４】同暗号化復号化装置において送受信認証手段を用いた場合のブロック図

【図５】同暗号化復号化装置におけるデータ用受信キーを同期データと共に送受信した場合のブロック図

＊【図６】本発明の実施の形態２における暗号化復号化装置の暗号化部のブロック図

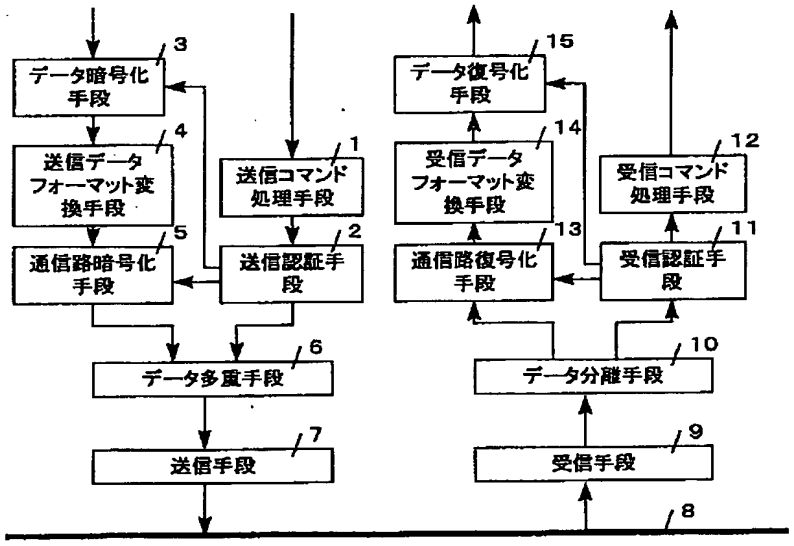
【図７】同暗号化復号化装置の復号化部のブロック図

【図８】従来の暗号化復号化装置のブロック図

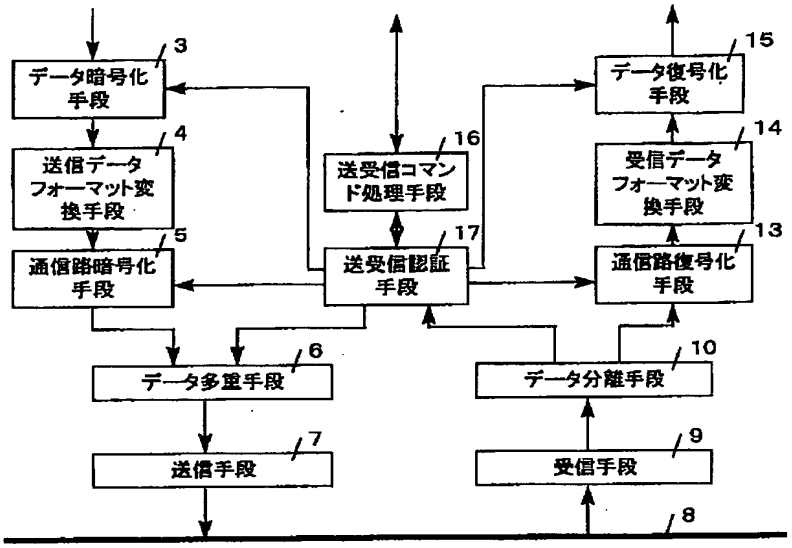
【符号の説明】

１　送信コマンド処理手段
２　送信認証手段
３　データ暗号化手段
４　送信データフォーマット変換手段
５　通信路暗号化手段
６　データ多重化手段
７　送信手段
８　伝送路
９　受信手段
１０　データ分離手段
１１　受信認証手段
１２　受信コマンド処理手段
１３　通信路復号化手段
１４　受信データフォーマット変換手段
１５　データ復号化手段

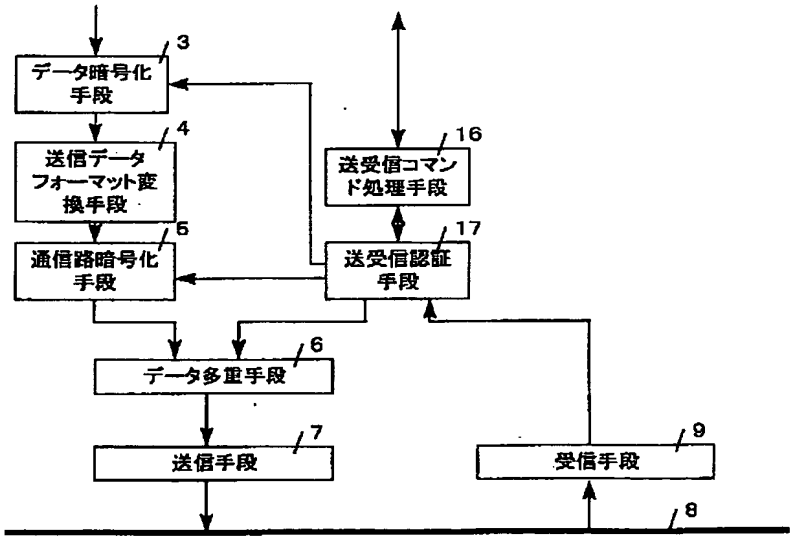
【図１】



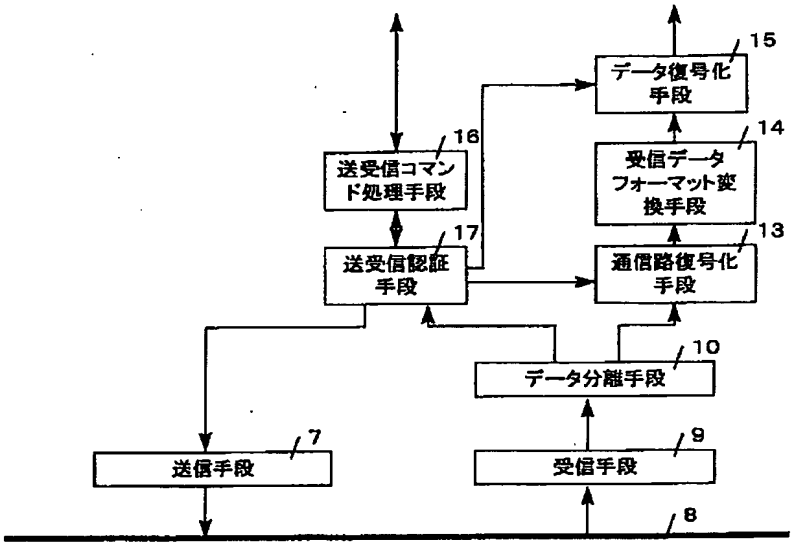
【図２】


データ暗号化手段
3
送信データフォーマット変換手段
4
通信路暗号化手段
5
データ多重手段
6
送信手段
7
送受信コマンド処理手段
16
送受信認証手段
17
データ復号化手段
15
受信データフォーマット変換手段
14
通信路復号化手段
13
データ分離手段
10
受信手段
9
8

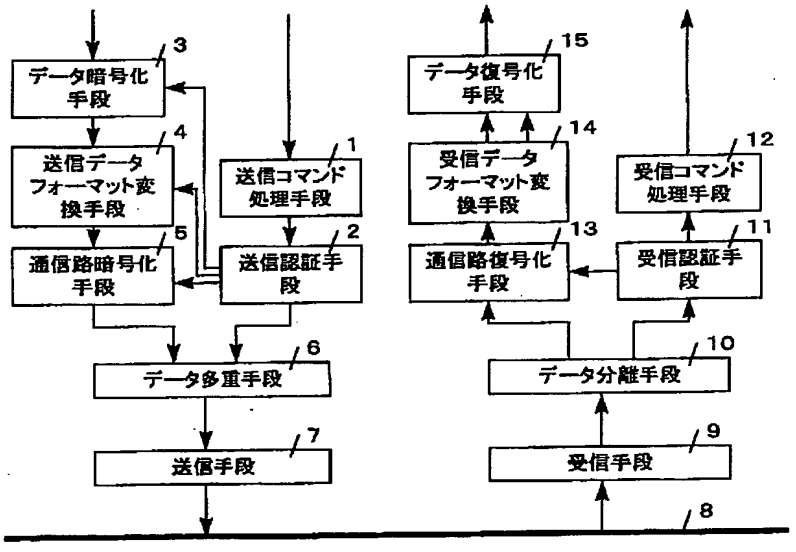
【図３】


データ暗号化手段
3
送信データフォーマット変換手段
4
通信路暗号化手段
5
データ多重手段
6
送信手段
7
送受信コマンド処理手段
16
送受信認証手段
17
受信手段
9
8

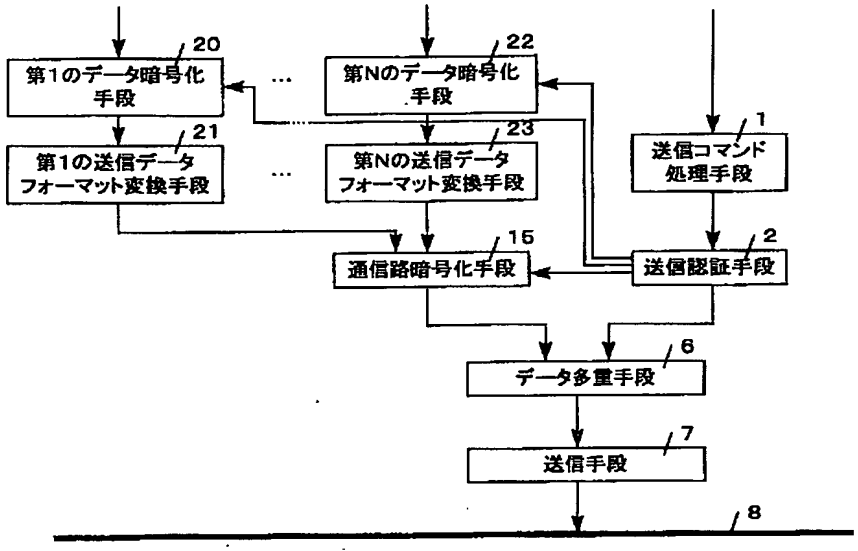
【図４】


データ復号化手段
15
受信データフォーマット変換手段
14
通信路復号化手段
13
送受信認証手段
17
送受信コマンド処理手段
16
データ分離手段
10
送信手段
7
受信手段
9
8

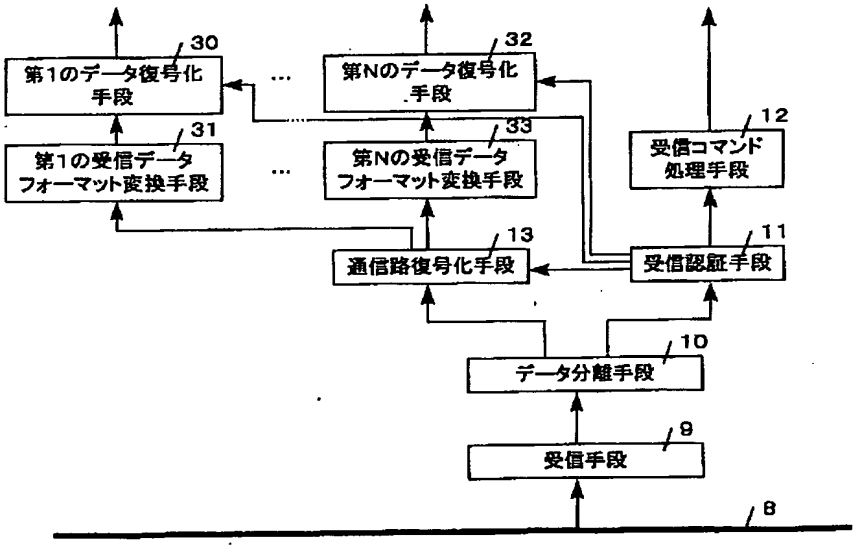
【図５】


データ暗号化手段
3
送信データフォーマット変換手段
4
通信路暗号化手段
5
送信コマンド処理手段
1
送信認証手段
2
データ多重手段
6
送信手段
7
データ復号化手段
15
受信データフォーマット変換手段
14
通信路復号化手段
13
受信コマンド処理手段
12
受信認証手段
11
データ分離手段
10
受信手段
9
8

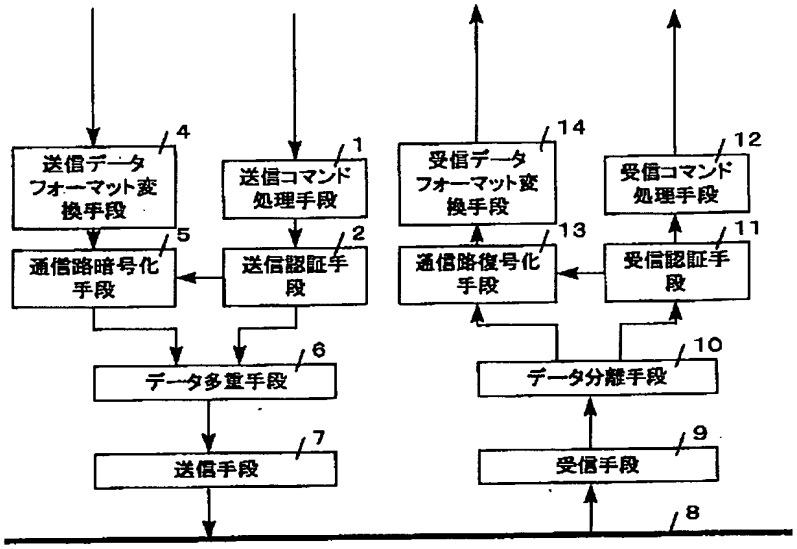
【図６】


20
第1のデータ暗号化手段
...
22
第Nのデータ暗号化手段
1
送信コマンド処理手段
21
第1の送信データフォーマット変換手段
...
23
第Nの送信データフォーマット変換手段
15
通信路暗号化手段
2
送信認証手段
6
データ多重手段
7
送信手段
8

【図７】


30
第1のデータ復号化手段
...
32
第Nのデータ復号化手段
12
受信コマンド処理手段
31
第1の受信データフォーマット変換手段
...
33
第Nの受信データフォーマット変換手段
13
通信路復号化手段
11
受信認証手段
10
データ分離手段
9
受信手段
8

【図８】



フロントページの続き

(72)発明者　小林　正明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　長岡　良富
大阪府門真市大字門真1006番地　松下電器産業株式会社内